PERFORMANCE AUDIT

OF

INFORMATION TECHNOLOGY SERVICES AND THE AUTOMATED INFORMATION SYSTEMS

BUREAU OF STATE LOTTERY

DEPARTMENT OF TREASURY

July 2002

EXECUTIVE DIGEST

INFORMATION TECHNOLOGY SERVICES AND THE AUTOMATED INFORMATION SYSTEMS

INTRODUCTION

This report, issued in July 2002, contains the results of our performance audit* of Information Technology Services and the Automated Information Systems, Bureau of State Lottery, Department of Treasury.

AUDIT PURPOSE

This performance audit was conducted as part of the constitutional responsibility of the Office of the Auditor General. Performance audits are conducted on a priority basis related to the potential for improving effectiveness* and efficiency*.

BACKGROUND

Information technology services are the responsibility of the Planning and Operations Division of the Bureau of State Lottery, Department of Treasury. The Division provides for the planning, testing, and evaluation of all on-line games and instant games; provides direct support for lottery retailers and all lottery retailer licensing functions; and provides all end-user computer support for the Bureau. The Division's mission* is to ensure that all services, standards, policies, and procedures fully satisfy the business information processing requirements of the Bureau.

The Bureau contracts with a third party vendor to provide the front-end communications network and gaming system

* *See glossary at end of report for definition.*

for the State's lottery. The Bureau's contractor is responsible for: installing and maintaining retailer sales terminals; maintaining a hot backup and recovery site* for both itself and the Bureau; running the distribution warehouse for instant tickets, on-line game supplies, and other retailer supplies; tracking all game processing transactions, including sales, rejections, cancellations, redemptions, and other validation attempts; calculating the retailer invoices weekly; and reporting to management. For fiscal year 2000-01, the Bureau and its contractor processed approximately $1.6 billion in ticket sales through their information systems.

The Bureau's information technology services function had expenditures of approximately $2.5 million and authorization for 38 full-time equated positions in fiscal year 2000-01.

AUDIT OBJECTIVES, CONCLUSIONS, AND NOTEWORTHY ACCOMPLISHMENTS

Audit Objective: To assess the effectiveness of general controls over the management and security of information processing.

Conclusion: The Bureau's general controls over the management and security of information processing were reasonably effective. However, we noted reportable conditions* related to a comprehensive information systems security program, operating system* access controls, operating system configuration, database* access controls, program change controls, and third party service organization* audits (Findings 1 through 6).

Noteworthy Accomplishments: The Bureau developed a comprehensive disaster recovery plan for its automated information systems. A documented disaster recovery plan is essential for ensuring continued operations in the

** See glossary at end of report for definition.*

event of a disruption. The Bureau's disaster recovery plan identified resources needed to recover from minor disruptions, such as the failure of a server, as well as major disasters that would require the Bureau to reestablish services at a backup location. During our audit, the Bureau conducted tests of its disaster recovery plan. We were informed that the Bureau was able to successfully restore operations at its backup site.

In addition, the Bureau established a quality assurance test laboratory. The Bureau uses the test laboratory to test program changes and new implementations of on-line and instant games prior to their release to the public. The test laboratory contains all of the hardware and software that the Bureau needs to replicate retailer sales activity and Bureau operations. Through the use of test plans and scripted procedures, the Bureau compares actual with expected test results to ensure that the games are functioning properly.

Audit Objective: To assess the internal control* and effectiveness of data input, processing, and output controls over the automated information systems.

Conclusion: The Bureau's internal control over the automated information systems was reasonably effective. However, we noted a reportable condition related to application access controls (Finding 7).

AUDIT SCOPE AND METHODOLOGY

Our audit scope was to examine the information processing and other records of the Bureau of State Lottery's automated information systems. Our audit was conducted in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States and, accordingly, included such tests of the records

** See glossary at end of report for definition.*

and such other auditing procedures as we considered necessary in the circumstances.

Our methodology included examination of the Bureau's and its contractor's information processing and other records for the period April 1999 through March 2002. Our methodology also included performing a risk assessment of the Bureau's and its contractor's automated information systems. We used this assessment to determine which systems to audit and the extent of our detailed analysis and testing. We reviewed the internal control over the Gaming System, On-Line Games System, Instant Games System, Financial System, and Retailer Licensing System pertaining to: (1) general controls, which included management and organization controls, program change controls, local area network* controls, and database controls, and (2) application controls, which included data input, processing, and output controls. We evaluated the results of our testing and reported our findings.

AGENCY RESPONSES

Our audit report contains 7 findings and 7 corresponding recommendations. The agency preliminary response indicates that the Bureau agreed with all the recommendations; however, it disagreed with Recommendation 1 as it relates to part b. of the finding.

** See glossary at end of report for definition.*

STATE OF MICHIGAN
OFFICE OF THE AUDITOR GENERAL
201 N. WASHINGTON SQUARE
LANSING, MICHIGAN 48913
(517) 334-8050
FAX (517) 334-8079

THOMAS H. MCTAVISH, C.P.A.
AUDITOR GENERAL

July 25, 2002

Mr. James E. Kipp, Acting Commissioner
Bureau of State Lottery
Department of Treasury
101 E. Hillsdale
Lansing, Michigan

Dear Mr. Kipp:

This is our report on the performance audit of Information Technology Services and the Automated Information Systems, Bureau of State Lottery, Department of Treasury.

This report contains our executive digest; description of agency; audit objectives, scope, and methodology and agency responses; comments, findings, recommendations, and agency preliminary responses; and a glossary of acronyms and terms.

Our comments, findings, and recommendations are organized by audit objective. The agency preliminary responses were taken from the agency's responses subsequent to our audit fieldwork. The *Michigan Compiled Laws* and administrative procedures require that the audited agency develop a formal response within 60 days after release of the audit report.

We appreciate the courtesy and cooperation extended to us during this audit.

Sincerely,

Thomas H. McTavish, C.P.A.
Auditor General

This page left intentionally blank.

TABLE OF CONTENTS

INFORMATION TECHNOLOGY SERVICES AND THE AUTOMATED INFORMATION SYSTEMS BUREAU OF STATE LOTTERY DEPARTMENT OF TREASURY

INTRODUCTION

	Page
Executive Digest	1
Report Letter	5
Description of Agency	8
Audit Objectives, Scope, and Methodology and Agency Responses	11

COMMENTS, FINDINGS, RECOMMENDATIONS, AND AGENCY PRELIMINARY RESPONSES

Effectiveness of General Controls	14
1. Comprehensive Information Systems Security Program	15
2. Operating System Access Controls	17
3. Operating System Configuration	20
4. Database Access Controls	21
5. Program Change Controls	23
6. Third Party Service Organization Audits	24
Internal Control Over Automated Information Systems	25
7. Application Access Controls	26

GLOSSARY

Glossary of Acronyms and Terms	28

Information Technology Services

Information technology services are the responsibility of the Planning and Operations Division of the Bureau of State Lottery, Department of Treasury. The Division provides for the planning, testing, and evaluation of all on-line games and instant games; provides direct support for lottery retailers and all lottery retailer licensing functions; and provides all end-user computer support for the Bureau. The Division's mission is to ensure that all services, standards, policies, and procedures fully satisfy the business information processing requirements of the Bureau.

The Bureau contracts with a third party vendor to provide the front-end communications network and gaming system for the State's lottery. The Bureau's contractor is responsible for: installing and maintaining retailer sales terminals; maintaining a hot backup and recovery site for both itself and the Bureau; running the distribution warehouse for instant tickets, on-line game supplies, and other retailer supplies; tracking all game processing transactions, including sales, rejections, cancellations, redemptions, and other validation attempts; calculating retailer invoices weekly; and reporting to management. For fiscal year 2000-01, the Bureau and its contractor processed approximately $1.6 billion in ticket sales through their information systems.

The Bureau's information technology services function had expenditures of approximately $2.5 million and authorization for 38 full-time equated positions in fiscal year 2000-01.

Automated Information Systems

During our audit period, the following automated information systems supported the Bureau's gaming operations:

1. Gaming System

   The Gaming System is the State's centralized gaming and reporting system. One of the System's primary functions is to process all game-related transactions. Authorized agents input gaming transactions into terminals installed by the contractor at their places of business. The System processes on-line and instant ticket wagers and validates winning tickets. In addition, the System provides other functions, such as managing and tracking instant ticket inventory. Accounting and marketing staff obtain information from the System to monitor retailer sales

histories and to manage the assignment of retailer sales terminals. The System also provides Bureau staff with information used to monitor and analyze System security and performance. Daily, the Bureau receives an electronic file of all transactions processed on the System.

2. On-Line Games System

The On-Line Games System is an automated system that the Bureau uses to process on-line ticket sales information received from its contractor. The System processes on-line ticket sales and validations for the Michigan Millions, Big Game, Rolldown, Daily 4, Daily 3, and Keno games; calculates retailer sales and commissions; and provides weekly sales reporting. In fiscal year 2000-01, the System processed approximately 2 to 4 million transactions daily and generated approximately $1 billion in gross revenues.

3. Instant Games System

The Bureau uses the Instant Games System to process instant ticket transactions using information received from its contractor. The System processes instant ticket sales for approximately 50 different instant games. The System also calculates instant ticket sales and commissions, tracks instant ticket inventory, and provides weekly sales reporting. In fiscal year 2000-01, the System processed approximately 300,000 transactions daily and generated approximately $600 million in gross revenues.

4. Financial System

The Financial System is used by the Bureau to process winning lottery payments from mail-in claims and large jackpots. The System interfaces winner payment information to the Michigan Administrative Information Network (MAIN) and produces W2G and 1099 information for transmittal to the Internal Revenue Service. In addition, the System uses information transferred from the On-Line Games and Instant Games Systems to calculate the amount of retailer's weekly electronic funds transfer (EFT) sweep. In fiscal year 2000-01, the Bureau of State Lottery collected $852 million in net receipts though the EFT process.

5. Retailer Licensing System

The Retailer Licensing System maintains business information and sales history for approximately 10,000 active retailers. The key functions of the System include retailer license application, approval, issuance, and renewals. Daily, new and

updated retailer information is interfaced from the Retailer Licensing System to the Gaming System. The Bureau's contractor uses the information to install and maintain retailer gaming terminals.

Audit Objectives, Scope, and Methodology and Agency Responses

Audit Objectives

Our performance audit of Information Technology Services and the Automated Information Systems, Bureau of State Lottery, Department of Treasury, had the following objectives:

1. To assess the effectiveness of general controls over the management and security of information processing.

2. To assess the internal control and effectiveness of data input, processing, and output controls over the automated information systems.

Audit Scope

Our audit scope was to examine the information processing and other records of the Bureau of State Lottery's automated information systems. Our audit was conducted in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States and, accordingly, included such tests of the records and such other auditing procedures as we considered necessary in the circumstances.

Audit Methodology

Our methodology included examination of the Bureau's and its contractor's information processing and other records for the period April 1999 through March 2002. Our audit fieldwork was performed between February 2001 and March 2002. To accomplish our audit objectives, our audit methodology included the following phases:

1. Preliminary Review and Evaluation Phase

   We identified the Bureau's and its contractor's automated information systems and performed a risk assessment of each system to determine those systems with the highest risk. Our risk assessment considered the critical nature of the information processed through each system as well as the number and dollar value of transactions processed. We used this assessment to determine the systems to audit and the extent of our detailed analysis and testing.

2. Detailed Analysis and Testing Phase

We reviewed the internal control over the Gaming System, On-Line Games System, Instant Games System, Financial System, and Retailer Licensing System pertaining to: (1) general controls, which included management and organization controls, program change controls, local area network controls, and database controls, and (2) application controls, which included data input, processing, and output controls. Specifically, we assessed:

a. Effectiveness of General Controls:

(1) We evaluated management and organization controls, including standards and procedures for data processing administration, computer operations, as well as system and data security. Also, we reviewed documentation relating to information system planning and risk assessments.

(2) We evaluated and tested controls over program changes, including documentation and the approval process.

(3) We observed and assessed controls over the local area network, including physical security, network access, operating system configuration, backup, and disaster recovery. Also, we reviewed network security assessments performed by third party contractors.

(4) We examined and evaluated database access controls and reviewed procedures for recovering the database in the event of a disaster.

b. Effectiveness of Internal Control Over Automated Information Systems:

(1) We evaluated controls over access and use of the Gaming System, On-Line Games System, Instant Games System, Financial System, and Retailer Licensing System.

(2) We assessed and documented the internal control over data input, data processing, and data output of the Gaming System, On-Line Games System, Instant Games System, Financial System, and Retailer Licensing System. Also, we conducted tests to determine whether the controls were working as intended.

3. Evaluation and Reporting Phase

   We evaluated and reported on the results of the preliminary review and evaluation phase and the detailed analysis and testing phase.

Agency Responses

Our audit report contains 7 findings and 7 corresponding recommendations. The agency preliminary response indicates that the Bureau agreed with all the recommendations; however, it disagreed with Recommendation 1 as it relates to part b. of the finding.

The agency preliminary response that follows each recommendation in our report was taken from the agency's written comments and oral discussion subsequent to our audit fieldwork. Section 18.1462 of the *Michigan Compiled Laws* and Department of Management and Budget Administrative Guide procedure 1280.02 require the Bureau to develop a formal response to our audit findings and recommendations within 60 days after release of the audit report.

COMMENTS, FINDINGS, RECOMMENDATIONS, AND AGENCY PRELIMINARY RESPONSES

EFFECTIVENESS OF GENERAL CONTROLS

COMMENT

Background: General controls are the policies and procedures that apply to all of the Bureau of State Lottery's automated information systems to help ensure their proper operation. The purpose of establishing general controls is to safeguard data, protect computer application programs, prevent unauthorized access to system software, and ensure continued computer operations in case of unexpected interruptions. The effectiveness of general controls is a significant factor in determining the effectiveness of application controls. Without effective general controls, existing application controls may be rendered ineffective by circumvention or modification.

Audit Objective: To assess the effectiveness of general controls over the management and security of information processing.

Conclusion: The Bureau's general controls over the management and security of information processing were reasonably effective. However, we noted reportable conditions related to a comprehensive information systems security program, operating system access controls, operating system configuration, database access controls, program change controls, and third party service organization audits.

Noteworthy Accomplishments: The Bureau developed a comprehensive disaster recovery plan for its automated information systems. A documented disaster recovery plan is essential for ensuring continued operations in the event of a disruption. The Bureau's disaster recovery plan identified resources needed to recover from minor disruptions, such as the failure of a server, as well as major disasters that would require the Bureau to reestablish services at a backup location. During our audit, the Bureau conducted tests of its disaster recovery plan. We were informed that the Bureau was able to successfully restore operations at its backup site.

In addition, the Bureau established a quality assurance test laboratory. The Bureau uses the test laboratory to test program changes and new implementations of on-line and instant games prior to their release to the public. The test laboratory contains all of

the hardware and software that the Bureau needs to replicate retailer sales activity and Bureau operations. Through the use of test plans and scripted procedures, the Bureau compares actual with expected test results to ensure that the games are functioning properly.

FINDING

1. Comprehensive Information Systems Security Program

The Bureau had not fully established a comprehensive information systems security program.

A comprehensive security program is the foundation of an entity's security control structure and a reflection of management's commitment to addressing security risks. The program should establish a framework for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. Without a well-designed program, security controls may be inadequate and inconsistently applied. Such conditions may lead to insufficient protection of critical resources or overexpenditures for controls over low-risk resources. A comprehensive security program should include periodic risk assessments, resources for independent monitoring of information systems' activity, and detailed policies and procedures for the safeguarding of all agency information system resources. Our review disclosed:

a. The Bureau had not performed a comprehensive security risk assessment for all aspects of its operations. Performing a comprehensive security risk assessment would help the Bureau identify threats that could adversely impact critical operations and assets. For example, the Bureau's risk assessment should identify areas of vulnerability related to personnel, facilities and equipment, communications, system software, operating systems, and applications. A risk assessment would also help to ensure that current and proposed safeguards are cost-effective, up to date, and responsive to threats.

   The Bureau had taken steps to identify and reduce certain risks. For example, the Bureau established policies and procedures related to information and data security and required its users to sign an acceptable use security agreement. Also, the Bureau requested this audit and contracted with another third party vendor to perform a network security review. In addition, the Bureau developed and successfully tested a disaster recovery plan. To

ensure that all significant threats are identified and corrected, the Bureau should conduct a formal risk assessment on a periodic basis or whenever conditions affecting its information system environment change.

b. The Bureau had not designated an independent information security officer. Instead, the Bureau had assigned the information system security function to the technical support manager, as well as the network and database administrators. Although these individuals have a role to play in maintaining the security of network and database resources, the overall security function should be independent. This would help ensure that the administrators' activities are appropriately monitored. Security officer duties include establishing a security program, developing and enforcing security policies and procedures, and monitoring system-recorded security activities and violations.

c. The Bureau's security program did not include the operating environment and information systems of its contractor. The Bureau contracts with a vendor to provide the front-end network and gaming system for the State's lottery. Our review of general and application controls of the contractor disclosed similar control weaknesses to those we identified at the Bureau. In addition, we determined that the contractor had not performed its own risk assessment to identify and reduce risks potentially affecting the security and integrity of software and data. Because the contractor is an integral part of the Bureau's operations, the Bureau should coordinate security activities with the contractor's management to ensure that security related issues, including those we identified, are appropriately addressed.

RECOMMENDATION

We recommend that the Bureau fully establish a comprehensive information systems security program.

AGENCY PRELIMINARY RESPONSE

The Bureau agreed with the recommendation as it relates to parts a. and c. of the finding. Regarding parts a. and c., the Bureau informed us that it would complete a more comprehensive risk assessment and will work with its contractor to implement additional controls. The Bureau disagreed with the recommendation as it relates to part b. of the finding. The Bureau does not believe it needs to establish an

independent security officer because of the checks and balances built into its manual and automated processes and the level of security awareness of its staff.

FINDING

2. Operating System Access Controls

The Bureau should improve operating system access controls.

Effective access controls protect information and resources from unauthorized modification, loss, or disclosure by restricting or detecting inappropriate access attempts. Access controls include restricting physical access and implementing logical controls that require users to authenticate themselves through the use of a unique user code and password or other personal identifier. For controls to be effective, access to data, program, and system files should be granted only to the extent necessary for individuals to perform their assigned duties. We identified the following access control weaknesses:

a. The Bureau did not sufficiently restrict access to super user privileges. We identified seven user and system accounts with super user capabilities. Individuals with access to the super user accounts or an equivalent level of privilege have the ability to manipulate and circumvent operating system and security controls. Super user privileges should be granted only to employees, such as the system administrator, who require privileged access* and who are specifically trained in the use of those privileges. The level of access granted to all other employees should not exceed the level required for them to perform their assigned duties. On some systems, users shared the super user account and password. Therefore, the Bureau could not establish individual accountability and monitor work performed.

b. The Bureau should strengthen its password control policy. Effective password controls for user and administrative accounts would help prevent unauthorized access and would help protect against potential password cracking attempts. The Bureau should expand its current password policy to include specific criteria for selecting passwords. Including specific criteria will help educate employees on how to select a secure password. In addition, the Bureau

* *See glossary at end of report for definition.*

should periodically perform tests to verify that users are complying with established policies.

c. The Bureau had not secured permissions on certain operating system, application, and data files. Access privileges to these files should be restricted to authorized users. We identified critical system files that could be read or modified by users or intruders that would allow them to bypass security controls. Securing sensitive files would reduce the risk that unauthorized activity could occur and sensitive information could be compromised. During the course of our review, the network administrator took steps to secure these files.

d. The Bureau did not routinely monitor its operating system logs. One of the most important tasks in keeping a computer system secure is monitoring the security of the system. This task requires the network administrator to routinely monitor log files for unauthorized access and other security related problems. Log files may provide the details of what is occurring, what systems are being attacked, and what systems have been compromised. The log files also provide useful information to monitor system performance and to track problems. As such, the log files should be regularly backed up and archived. Because of the large volume of information captured by the various system logs, the Bureau may wish to use custom scripts, operating system utilities, or third party software to assist in the identification of critical system events.

e. The Bureau had not established a formal process for documenting user requests for system access or for monitoring existing access. The Bureau's managers are responsible for requesting the appropriate level of access for their staff and for notifying technical support when a user's access is no longer needed. However, we identified 22 network accounts for which access was no longer needed. Deleting or disabling these accounts would reduce the risk of unauthorized system access. Subsequent to our inquiry, the network administrator disabled the accounts.

f. The Bureau did not ensure that suitable security banners were displayed at all computer access points to the network. The security banner should expressly prohibit unauthorized access and remove identifying information about the Bureau's operating systems. The systems should be configured to limit the amount of information that is made available to unidentified individuals

because potential intruders could use this information to identify vulnerabilities of the operating systems that would assist in an attack. Upon bringing this matter to the Bureau's attention, the Bureau strengthened its warning message and removed information about its operating systems.

g. The Bureau did not restrict the workstations from which privileged accounts could log on to the system. The operating system has the ability to restrict users from logging on as the super user on any workstation other than the console. Legitimate users with knowledge of the super user password would still be able to switch to the super user account after first logging on with their own account. This control would provide an extra layer of protection and accountability. In addition, the Bureau did not automatically disconnect users from the network or use password-protected screen savers after a reasonable period of inactivity. This could result in unauthorized system access if a workstation is left unattended. Department of Management and Budget Administrative Guide procedure 1310.02 requires that workstations automatically log off if left unattended for a specific period of time.

h. The Bureau did not restrict access to the computer room. The Bureau granted access to over 18 individuals who did not require access for their job responsibilities. This included Application Development staff with specialized knowledge that would allow them to bypass established controls. The Bureau had also granted access to other personnel who had no need for access, such as Administration and Retailer Services staff. Effectively restricting access to the computer room and having operations personnel accompany and oversee all other personnel granted access would help prevent unauthorized use of the computer system and interference with computer operations.

RECOMMENDATION

We recommend that the Bureau improve operating system access controls.

AGENCY PRELIMINARY RESPONSE

The Bureau agreed with the recommendation and informed us that it has taken steps to improve operating system access controls. In addition, the Bureau is continuing to investigate ways to eliminate the need for its computer operations to have privileged access.

FINDING

3. Operating System Configuration

The Bureau had not fully established controls and documentation for network operating system configurations. The proper configuration of operating systems is important to ensure the reliable operation of computers and the continuous availability and integrity of critical information.

An operating system should be installed with the minimum services required to support business operations. We identified unnecessary services that were installed by default. Many of these services have known exploits and vulnerabilities associated with the services. Removing or disabling these services would reduce the risk that an unauthorized user could gain access to the system or target the system for a denial of service attack.

In addition, we identified parameters in other configuration files that were not properly secured. An unauthorized user could exploit these weaknesses to gain access to the operating system, application programs, and data.

During our review, the Bureau took steps to address the identified configuration weaknesses. However, to further improve controls, the Bureau should establish policies and standards for configuring its operating systems. The policies and standards should identify critical and sensitive operating system files and establish a baseline configuration for the files. Documenting and establishing a baseline configuration will help ensure that all systems are configured securely and will aid in the detection of unauthorized changes to the system.

RECOMMENDATION

We recommend that the Bureau fully establish controls and documentation for network operating system configuration.

AGENCY PRELIMINARY RESPONSE

The Bureau agreed with the recommendation and informed us that it had secured the operating system configuration files. In addition, the Bureau informed us that it would establish policies and standards for configuring its operating systems.

FINDING

4. Database Access Controls

The Bureau should improve its database access controls. Effective controls help prevent or detect inappropriate access to the Bureau's data, thereby protecting the data from unauthorized modification, loss, or disclosure.

Our review disclosed:

a. The Bureau did not sufficiently restrict operating system accounts with privileged access to the database. Users with privileged access have access to all data and have the ability to bypass established security controls. Therefore, users with privileged access could intentionally or inadvertently make changes to the database affecting security or performance. Our review identified seven accounts with privileged access. After we brought this matter to management's attention, the Bureau took steps to remove the access for all but one of the accounts in question. We were informed that the Bureau is working on a solution to eliminate the need for the remaining group to have this level of access.

b. The Bureau had not established or changed passwords on all default database accounts. We identified two accounts for which the password had not been established or changed from the default. Changing the password on default accounts is critical because default accounts are usually the first accounts tried by an intruder attempting to break into a system. After we brought this matter to management's attention, the Bureau took steps to correct the problem.

c. The Bureau's analysts had been granted privileged access to database tables. We were informed that the analysts had this access to correct data errors that could not be corrected through the application. The Bureau could improve controls by granting and then revoking the privileged access after each data correction is performed. In addition, database audit logs* should be used to monitor privileged access and ensure that data corrections are made as directed by management.

* *See glossary at end of report for definition.*

d. Database administrators (DBAs) did not perform their work using a unique database administration account. Currently, DBAs perform their work using a shared database administration account. DBAs need privileged access to perform their administration duties. The sharing of accounts prevents management from effectively monitoring and assigning responsibility for these privileged activities. DBAs have unique user accounts with lesser privileges that they use to perform nonprivileged work. DBAs could create and assign to themselves a privileged role to use when performing DBA duties.

e. The Bureau did not sufficiently restrict access to sensitive database system files and database tables. Access to these files and tables should be restricted to DBAs. Unauthorized users could use information contained in the files and tables to bypass established controls, thereby affecting the availability or integrity of the system.

f. The Bureau should strengthen its database password rules and other log-in parameters. Effective password controls are one of the primary means to prevent unauthorized access to information resources. To improve security, the Bureau should take advantage of database password and log-in security features.

g. The Bureau did not use database audit logs to monitor sensitive database activity. Audit logs can be configured to automatically record privileged access, data corrections, or other sensitive activity for management review. Audit logs also provide management with the means to identify unauthorized activity. The Bureau should identify sensitive activity and develop the means to monitor it.

RECOMMENDATION

We recommend that the Bureau improve its database access controls.

AGENCY PRELIMINARY RESPONSE

The Bureau agreed with the recommendation. The Bureau informed us that it is taking steps to improve database access controls, such as investigating a means to further limit privileged access and developing a means to audit and monitor sensitive activity and strengthen database password rules.

FINDING

5. Program Change Controls

The Bureau had not completely established controls over program changes.

It is important for an organization's information security to ensure that only authorized and fully tested software is placed in operation. This is accomplished by ensuring that all changes are properly documented, authorized, and tested and that access to programs and movement of programs to production are controlled. Our review disclosed:

a. The Bureau did not sufficiently secure access to script files used to promote source code files from development to production. The Bureau's Production Control staff and Operations staff use a series of script files to access source code files, move the files to the appropriate production directory, compile the source code, and then transfer the compiled code to the proper application server. We determined that the permissions on these files were such that the Application Development staff or other unauthorized users could access and execute the scripts, thereby promoting an unapproved program change.

b. The Bureau did not maintain testing documentation for program changes. In addition, end users gave verbal approval that test results were satisfactory and met the requirements documented in the change request. We selected and reviewed documentation for 15 program changes. For 13 (87%) of 15 program changes, testing documentation was not maintained. None of the 15 program changes had documentation to support end user approval and sign-off of the project. We were informed that the end users approved the changes verbally. Documenting test results and end user approvals is necessary to help ensure that program changes are properly tested and meet users' needs.

c. The Bureau did not maintain previous versions of application source code on the network. When Production Control moves a modified program into production, the new program writes over the existing program. Currently, the only way to obtain a previous version is from the network backup tapes or to rekey the source code from hard copy. Without maintaining previous program versions that can serve as an audit trail, the Bureau's programmers cannot easily re-create a previous version of the file and the project's history.

d. The Bureau had not established automated program version controls, including numbered program versions and a history of program changes. Library control software is often used to provide these types of controls. In addition, library control software would provide a mechanism for programmers to check in and check out production source code and provide a means for management to log and monitor when source code was copied or changed. During our audit period, the Bureau was in the process of modifying and testing library control software.

RECOMMENDATION

We recommend that the Bureau completely establish controls over program changes.

AGENCY PRELIMINARY RESPONSE

The Bureau agreed with the recommendation and informed us that it has restricted access to the script files used to promote source code files from development to production. The Bureau will modify documentation standards to include the retention of test results and end user sign-offs. In addition, the Bureau is implementing change control software that will provide version control and a history of program changes.

FINDING

6. Third Party Service Organization Audits

The Bureau should take steps to ensure the operating effectiveness of the internal control of third party service organizations that impact its financial statements.

The Bureau contracts with a vendor to provide electronic data processing of instant and on-line lottery ticket transactions. As a result, transactions affecting the Bureau's financial statements are subject to internal controls that are physically and operationally separate from the Bureau's own internal controls.

Act 431, P.A. 1984, as amended by Act 8, P.A. 1999, requires each State department and sub-unit to establish and maintain an internal control structure using generally accepted accounting principles and directives from the Office of Financial Management. Therefore, the Bureau should obtain assurances that the internal control structure of its contractor is sufficient to ensure that the financial

information reported is materially correct and that assets are properly safeguarded. This assurance can be obtained from an audit of the third party service organization. This type of audit is described in the American Institute of Certified Public Accountants Statement on Auditing Standards (SAS) No. 70 and is commonly referred to as a SAS 70 audit. There are two types of SAS 70 audits. The first type is a report on controls placed in operation by the third party service organization. The second type is a report on the controls placed in operation by the third party service organization and tests of operating effectiveness of those controls. The second type is preferable because it provides management with more assurance as to the effectiveness of the service organization's internal control over a period of time.

The Bureau's contract provides for an annual review of the vendor's operations at the Bureau's request.

RECOMMENDATION

We recommend that the Bureau take steps to ensure the operating effectiveness of the internal control of third party service organizations that impact its financial statements.

AGENCY PRELIMINARY RESPONSE

The Bureau agreed with the recommendation and informed us that it would consider requiring a SAS 70 audit of the contractor. However, the current budget shortage may impact the feasibility of requesting this type of audit in the near term.

INTERNAL CONTROL OVER AUTOMATED INFORMATION SYSTEMS

COMMENT

Background: Application controls are directly related to specific computer applications. They help ensure that transactions are valid, properly authorized, completely and accurately processed, and reported. Application controls include automated control techniques, such as computer edits, and manual techniques, such as reviews of reports identifying rejected or unusual items.

Audit Objective: To assess the internal control and effectiveness of data input, processing, and output controls over the automated information systems.

Conclusion: The Bureau's internal control over the automated information systems was reasonably effective. However, we noted a reportable condition related to application access controls.

FINDING

7. Application Access Controls

The Bureau had not established control procedures to prevent unauthorized users from accessing and using its automated information systems.

We reviewed user access to the On-Line Games System, Instant Games System, Financial System, and Retailer Licensing System. Our review disclosed:

a. The Bureau did not assign access rights to only those users requiring access for their job responsibilities. Access to the Bureau's automated information systems is controlled by a security application. Users are granted access to the various system screens based on transaction codes defined in the security application. A transaction code controls the type of access the user has in the system, such as whether the user has read-only access or the ability to add, modify, or delete transactions. We reviewed user access to 29 transaction codes used to manage retailer or winner information. For 14 (48%) transaction codes, we identified users who did not require access to the transaction for their job function. In some instances, this was caused because a transaction code had multiple screens and incompatible functions associated with it. The Bureau should review its users' access needs and adjust their access rights accordingly.

b. The Bureau did not restrict the access of its Application Development staff to production transactions. We identified 23 (79%) of 29 transactions in which the Bureau's programmers had update capabilities. Sound internal control requires that production data be accessed and changed only by authorized users and that programmers access only test data. Restricting access to production data or establishing compensating controls, such as a means to monitor transactions processed by the Application Development staff, will help ensure the integrity of the data.

c. The Bureau had not established formal policies and procedures for periodically reviewing users' access to its automated information systems and for removing access that is no longer needed. We were informed that the Bureau is in the process of developing reports to enable its managers to periodically review access to its automated information systems. We identified nine accounts that were for users who had left the Bureau's employment or that were no longer needed. The risk of unauthorized access was minimized because the Bureau had disabled these accounts at the operating system level. However, formal procedures would help the Bureau manage its users' access and ensure that only authorized users had access to its automated information systems.

RECOMMENDATION

We recommend that the Bureau establish control procedures to prevent unauthorized users from accessing and using its automated information systems.

AGENCY PRELIMINARY RESPONSE

The Bureau agreed with the recommendation and informed us that it is developing formal policies and procedures to review user access rights. In addition, the Bureau will establish a means to monitor transactions processed by its Application Development staff as a compensating control.

Glossary of Acronyms and Terms

audit log	An audit trail of computer system activity (e.g., files accessed, jobs processed, and commands entered into a computer console).
database	A program that manages data and can be used to store, retrieve, and sort information.
DBA	database administrator.
effectiveness	Program success in achieving mission and goals.
efficiency	Achieving the most outputs and outcomes practical with the minimum amount of resources.
EFT	electronic funds transfer.
hot backup and recovery site	A fully operational off-site data processing facility equipped with both hardware and system software to be used in the event of a disaster.
internal control	The organization, policies, and procedures adopted by agency management and other personnel to provide reasonable assurance that operations, including the use of agency resources, are effective and efficient; financial reporting and other reports for internal and external use are reliable; and laws and regulations are followed. Internal control also includes the safeguarding of agency assets against unauthorized acquisition, use, or disposition.
local area network (LAN)	A series of interconnected computers, printers, and other computer equipment that share hardware and software resources. The service area is usually limited to a given floor, office area, or building.

mission	The agency's main purpose or the reason that the agency was established.
operating system	The main control program of a computer. The operating system controls all of the computer's resources and provides the base upon which other application programs can be used or written.
privileged access	Extensive system access capabilities granted to individuals responsible for maintaining system resources. This level of access is considered high risk and must be controlled and monitored by management.
performance audit	An economy and efficiency audit or a program audit that is designed to provide an independent assessment of the performance of a governmental entity, program, activity, or function to improve public accountability and to facilitate decision making by parties responsible for overseeing or initiating corrective action.
reportable condition	A matter that, in the auditor's judgment, represents either an opportunity for improvement or a significant deficiency in management's ability to operate a program in an effective and efficient manner.
service organization	The entity that provides services to the user organization.